TRANSMITTAL OF APPEAL BRIEF

Docket No.
VID-01602/29

In re Application of: Barry H. Schwab et al.

Application No.	Filing Date	Examiner	Group Art Unit
09/877,596-Conf. #1588	June 8, 2001	L. T. Jacobs	2457

Invention: METHOD FOR SECURE TRANSACTIONS UTILIZING PHYSICALLY SEPARATED COMPUTERS

TO THE COMMISSIONER OF PATENTS:

Transmitted herewith is the Appeal Brief in this application, with respect to the Notice of Appeal filed: November 8, 2010 . and Pre-appeal Brief Review Panel Decision dated Dec. 21, 2010.

The fee for filing this Appeal Brief is $ 270.00 .

☐ Large Entity ☒ Small Entity

☐ A petition for extension of time is also enclosed.

The fee for the extension of time is _____ .

☐ A check in the amount of _____ is enclosed.

☐ Charge the amount of the fee to Deposit Account No. _____ .

☒ Payment by credit card.

☒ The Director is hereby authorized to charge any additional fees that may be required or credit any overpayment to Deposit Account No. 07-1180 .
This sheet is submitted in duplicate.

_____ Dated: January 21, 2011

John G. Posa
Attorney Reg. No. : 37,424
GIFFORD, KRASS, SPRINKLE, ANDERSON & CITKOWSKI, P.C.
2701 Troy Center Drive, Suite 330
Post Office Box 7021
Troy, Michigan 48007-7021
(734) 913-9300

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BOARD OF PATENT APPEALS AND INTERFERENCES

In re application of: Schwab et al.

Serial No.: 09/877,596 Group No.: 2157

Filed: June 8, 2001 Examiner: L. Jacobs

For: METHOD FOR SECURE TRANSACTIONS UTILIZING PHYSICALLY SEPARATED COMPUTERS

APPELLANTS' APPEAL BRIEF UNDER 37 CFR §41.37

Mail Stop Appeal Brief
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Dear Sir:

I. Real Party in Interest

The real parties in interest in this case are Barry H. Schwab and John G. Posa, individuals, Applicants and Appellants.

II. Related Appeals and Interferences

A previous appeal led to a Board Decision dated May 24, 2010.

III. Status of Claims

The present application was filed with 12 claims. Claims 13-15 were added by RCE amendment in July 2010. Claims 1-15 are pending, rejected and under appeal. Claim 1 is the sole independent claim.

IV. Status of Amendments

No after-final amendments have been submitted.

V. Summary of Claimed Subject Matter

Independent claim 1 is directed to a secure transaction method beginning with the step of establishing an electronically accessible verification site authorized by the holder of a credit card (Specification, page 3, line 16 to page 4, line 3). A request for goods or services is received by a merchant using the credit card; however, the card is not required to be physically presented to the merchant (Specification, page 2, lines 13-15). The verification site is accessed by the merchant to determine whether the request for goods or services is an authorized transaction (Specification, page 4, lines 4-21). An electronic authorization communication is sent by the verification site to the holder of the credit card. This message includes information indicative of the transaction. If the transaction is approved by the card holder, that person or entity sends an approval communication (Specification, page 4, lines 4-12).

VI. Grounds of Rejection To Be Reviewed On Appeal

A. The rejection of claim 1 under 35 U.S.C. §102(e) as being obvious in view of U.S. Publ. No. 2001/0027527 to Khidekel *et al.* ("Khidekel") in view of U.S. Publication No. 2001/0051902 to Messner.

B. The rejection of claim 2 under 35 U.S.C. §102(e) over Khidekel in view of Messner.

C. The rejection of claim 3 under 35 U.S.C. §102(e) over Khidekel in view of Messner.

D. The rejection of claim 4 under 35 U.S.C. §102(e) over Khidekel in view of Messner.

E. The rejection of claim 5 under 35 U.S.C. §102(e) over Khidekel in view of Messner.

F. The rejection of claim 6 under 35 U.S.C. §102(e) over Khidekel in view of Messner.

G. The rejection of claim 7 under 35 U.S.C. §102(e) over Khidekel in view of Messner.

H. The rejection of claim 8 under 35 U.S.C. §102(e) over Khidekel in view of Messner.

I. The rejection of claim 9 under 35 U.S.C. §102(e) over Khidekel in view of Messner.

J. The rejection of claim 10 under 35 U.S.C. §102(e) over Khidekel in view of Messner.

K. The rejection of claims 11 and 12 under 35 U.S.C. §102(e) over Khidekel in view of Messner.

L. The rejection of claim 13 under 35 U.S.C. §102(e) over Khidekel in view of Messner.

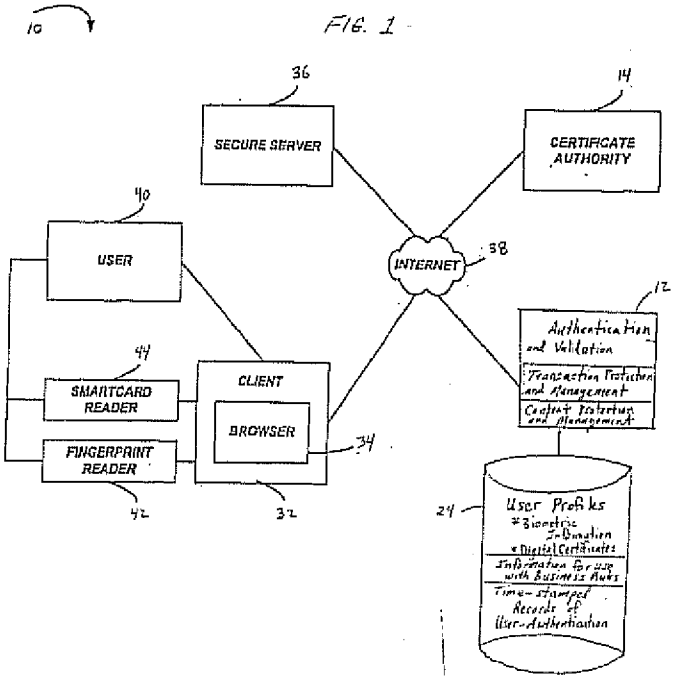
M. The rejection of claim 14 under 35 U.S.C. §102(e) over Khidekel in view of Messner.

N. The rejection of claim 15 under 35 U.S.C. §102(e) over Khidekel in view of Messner.

VII. Argument

The Teachings of Khidekel

Making reference to Figure 1 of the Khidekel publication, Khidekel resides in a system that permits secure communications between a client device 32 executing a browser 34, and a secure server 36 over a public network 38 such as the Internet. "Authentication can be ensured not only of the client 34, but also of the user 40." (Khidekel, [0027])



To use the system of Khidekel, a potential user must first go through an enrollment process. (Khidekel, [0020]) In accordance with one disclosed example, a hospital administrator can establish user accounts and enroll users directly. Alternatively, each user may be supplied with a one-time password that allows the user to enroll in the system. Initial enrollment may require that the user

provide biometric information, for example, a fingerprint, as indicated by the enrollment page in FIG. 3. The information provided by the administrator, as well as profiles of the users, is sent to the server 12 where it can be encrypted and stored in a database 24 (FIG. 1). Personal information about the users, including user preferences and user credentials can be maintained in encrypted form in the database 24 (see Figure 1, above) (Khidekel, [0020])

Following enrollment, a user may gain access to "secure server" (36) and the services which it provides by being authenticated by authentication server 12. Examples of services 56 that can be accessed only after authentication by the server 12 are illustrated in FIG. 2 (below). The services can include secure electronic mail (email), notary services, contract management, calendaring and access to a digital vault. Similarly, access to financial accounts, person-to-person payment services, trading services, electronic bill services, electronic wallet shopping services, investor services, travel services and other services can be provided through the portal 52. "Prior to using the services 56, the user's credentials would be submitted to the server 12 for authentication." (Khidekel, [0023])

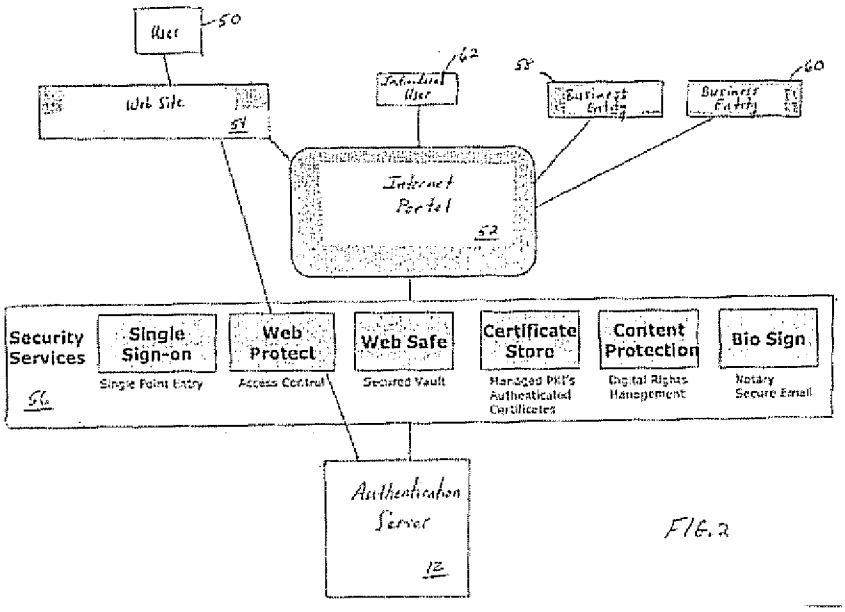


FIG. 2

If a user is properly authenticated, the authentication server 12 generates a token 90 (See Figure 5 of Khidekel) which encodes the user's login name and the name or other identification of the secure server 36. Upon receiving the token 90, the secure server 36 validates the token by comparing 72 the

difference between the current time and the authentication time to a predefined threshold. For example, a hospital might define the threshold as one month. (Khidekel, [0035]-[0036]) Depending on the structure of the systems, it may be necessary to provide a token for each server to be accessed, thereby resulting in multiple tokens being issued (Khidekel, [0037]).

Appellants request that the Board keep the following points about the Khidekel system in mind:

1. Once a user has been authenticated and has been issued the token (or tokens), *there is no direct involvement in authorizing the specific transactions that later are conducted by the user*;

2. Although the system may require the user to be re-authenticated later in the transaction process, *it is the user that is approved*, not the transaction;

3. Khidekel is an access control system, which is not related to any specific activities after the access has been granted, and which teaches away from participation in the details of any specific transaction that occurs once access is allowed; and

4. Although Khidekel envisions ecommerce transactions (see [0023] and Figure 2 of Khidekel), there is no mention of users holding credit cards or merchants accepting them.

The Teachings of Messner

Messner discloses two methods for authenticating a transaction prior to approval. In the first method ("Split Transaction Model" [0083]-[0089]; Fig. 9A, 9B), the authorization is transmitted *simultaneously with the order information*. In accordance with the second method ("Interactive Client Approval Model" [0090]-[0007]; Fig. 10A, 10B), the user is required to provide a confirmation of the order, but the approval is performed through a specific channel; namely, the user client system.

With regard to Messner, Appellants respectfully request that the Board take note of the following:

1. The first method, the Split Transaction Model is clearly different from Appellants' claimed invention, in which the authorization is transmitted after the order is submitted;

2. All methods of Messner require the use of a pre-determined communication path/method (typically via a third-party or a user-designated e-mail account). The system essentially assumes that an order received from a particular client computer has been issued by the user himself or herself;

3. With regard to the second method—the Interactive Client Approval Model—although

Messner specifies that the request is transmitted to the user client system by way of IP addresses, this is impractical unless the step is performed contemporaneous to the transaction. IP addresses on typical connections (such as dial-up service, or broadband services provided by various Cable or Telephone service providers) are assigned dynamically using systems such as DHCP, and thus are not persistent. If a user were to log in over a wireless connection, and then switch to a separate wired connection after arriving at home, then there is essentially no possibility that the two sites would be assigned the same IP addresses. It is only by staying on-line throughout the entire authentication/authorization process that this approach would be usable. In addition, the path chosen would not allow the user to specify the communications path and method to be utilized, as that has been pre-determined by the system of Messner.

A. The Rejection of Claim 1.

In addition to deficiencies regarding the lack of credit card usage, the Examiner concedes that Khidekel fails to disclose Appellants' steps of:

> sending an electronic authorization communication by the verification site to the holder of the credit card, the message including information indicative of the transaction; and
>
> transmitting, by the holder of the credit card, an approval communication if the transaction is approved by the card holder.

Based upon the teachings of Messner, the Examiner argues that it would be obvious to modify the system of Khidekel "by generating an authorization packet that includes biometric information for approving a transaction securely over a network." (Final OA, page 3). For the following reasons, Appellants respectfully disagree:

1. The limitations of claim 1 in question have nothing to do with "generating an authorization packet that includes biometric information."

2. Khidekel has nothing to do with direct approval of *a transaction* by a user, particularly on a transaction-by-transaction basis. The teachings of Messner notwithstanding, the system of Khidekel is detailed, complete, and specifically directed to user enrollment and authentication. In fact, as discussed above, Khidekel teaches away from additional user involvement in the authentication process following enrollment. The entire point of Khidekel is to off-load the user from additional

authentication following enrollment by storing user profiles in database (24) so that when a user requests secure services, the authentication server 12 can "take over," thereby alleviating the user from transaction approval, for example.

3. Even if Khidekel were "modified" by Messner, the proposed combination does not teach or suggest transmitting an approval communication by a card holder *after* a request for goods or services is submitted. In the embodiments of Messner, approval occurs contemporaneously with a user request, either explicitly under the Split Transaction Model, or implicitly under the Interactive Client Approval Model.

4. Khidekel specifies the use of a token (or tokens), whereas the instant invention has no element of a token to be used to control access, and, in fact, does not concern itself with the specifics of how a connection path is established. Messner uses no tokens, and has no obvious way to integrate the use of one in the methods as disclosed.

In partial summation, because the systems of Khidekel and Messner specify authorization to occur at different points in the transaction process (and Khidekel specifies only access control, and not participation in specific transactions) there is no motivation to combine these two references. Furthermore, the systems of Khidekel and Messner provide no user control of the communication path to be utilized, or for the method to be used for requesting and confirming authorization for a specific transaction. Accordingly, *prima facie* obviousness has not been established.

B. Claim 2.

Khidekel does not teach that the verification site is an electronic mail account. Rather, in [0025], Khidekel states that "[o]nce the administrator subscribes, the system generates a shared electronic key and a random password that are delivered to the administrator by certified mail or in some other secure manner." This is not the same as *establishing a verification site*.

C. Claim 3.

Paragraphs [0020] and [0025] of Khidekel do not disclose an electronic mail account functioning as a verification site having been established by a merchant.

D. Claim 4.

Paragraphs [0020] and [0039] of Khidekel do not disclose that an authorization message is sent from the verification site to the merchant in response to the step of accessing the verification site by the merchant.

E. Claim 5.

Appellants' claim 5 adds to claim 4 that the authorization message (sent from the verification site to the merchant in response to the step of accessing the verification site by the merchant) is automatically generated. The Examiner concedes that this is not disclosed by Khidekel (Final OA, top of page 4), but argues that this would be obvious in view of Messner ***under the identical rationale used to reject claim 1***; namely, that it would allow Khidekel to generate an authorization packet that includes biometric information for approving a transaction securely over a network. Appellants repeat the arguments made in rebuttal of the rejection of claim 1, reminding that claim 5 adds the limitations of claims 5 *and 4* to claim 1, such that the same reasons for rejection cannot reasonably apply.

F. Claim 6.

Claim 6 adds to claim 1 that the authorization message *is manually generated* within a predetermined period of time. Admitting that such a step is not suggested by Khidekel, the Examiner argues that it would be obvious to modify Khidekel "by manually generating an authorization packet that includes biometric information for approving a transaction securely over a network." Not only has the Examiner once again "cut and pasted" the same rejection used for claims 1 and 5, neither Khidekel nor Messner would take advantage of such a step since neither have anything to do with a card holder approving a transaction after the fact. Both Khidekel and Messner are directed to different types of automated processes, and teach away from Appellants' claimed user-merchant interactions.

G. Claim 7.

Although Khidekel considers encryption (*See*, Khidekel at [0008]), Appellants' claim 7 is dependent upon claim 4, and should be deemed allowable for the reasons presented above.

H. Claim 8.

Khidekel does not teach or suggest encryption implemented using an algorithm specific to the holder or an authorized user of the card, and the Examiner provides no citations in support of the rejection.

I. Claim 9.

Paragraph [0023] of Khidekel does not teach or suggest, in combination with the limitations of Appellants' claim 4, that the step of accessing the verification site, the authorization message, or any combination thereof, include routing information for future use. Paragraph [0023] of Khidekel reads as follows:

> "Examples of services 56 that can be accessed only after authentication by the server 12 are illustrated in FIG. 2. The services can include secure electronic mail (email), notary services, contract management, calendaring and access to a digital vault. Similarly, access to financial accounts, person-to-person payment services, trading services, electronic bill services, electronic wallet shopping services, investor services, travel services and other services can be provided through the portal 52. Prior to using the services 56, the user's credentials would be submitted to the server 12 for authentication."

This paragraph does not mention routing information for future use.

J. Claim 10.

Paragraphs [0025]-[0026] of Khidekel does not teach or suggest that the step of accessing the verification site by the merchant causes an icon or window to appear in a web browser. Paragraphs [0025]-[0026] of Khidekel discuss how a hospital administrator can subscribe to the security services offered through the web site. These paragraphs do not mention "icon" or "browser."

K. Claims 11 and 12.

Paragraph [0019] of Khidekel states that the authentication server 12 interacts with enabled client devices 32, such as personal computers, wireless devices and personal digital assistants (PDAs). does not disclose that verification site is wirelessly accessible. However, Appellants' claims 11 and 12 are dependent upon claim 1, which includes the limitations of sending an electronic authorization

communication *by the verification site to the holder of the credit card*, the message including information indicative of the transaction. Such subject matter, in combination, is not disclosed or considered by Khidekel.

L. Claim 13.

Paragraphs [0019]-[0020] do not identify a merchant. These passages state only that the services provided by the authentication server 12 can be implemented, for example, either as an independent, central service or as a licensed software suite provided to individual businesses or organizations, and that the services provided by the authentication server 12 can be implemented as part of a secure transaction system in any one of several business models. Nothing is said about *merchant identification.*

M. Claim 14.

Paragraphs [0019]-[0020] do not identify goods or services. These passages state only that the services provided by the authentication server 12 can be implemented, for example, either as an independent, central service or as a licensed software suite provided to individual businesses or organizations, and that the services provided by the authentication server 12 can be implemented as part of a secure transaction system in any one of several business models. Nothing is said about information indicative of a transaction including information identifying the goods or services.

N. Claim 15.

The Examiner concedes that Khidekel is silent with respect to information indicative of a transaction including the cost of the transaction. The Examiner proposes to modify Khidekel with Messner "to generate an order packet that includes purchase information for the goods/services to be purchased and approving the transaction over a network." (Final OA, bottom of page 6). Khidekel has no need to convey cost information since Khidekel approves users and not transactions. Indeed, while Khidekel mentions services, it does not consider goods. Appellants claim 15 is not directed to generating an order packet that includes purchase information for the goods/services to be purchased." Rather, the claim is directed to *the cost of the transaction* (after a transaction is initiated). As such, the Examiner's reason for the rejection does not have a nexus to the claim language in question.

Conclusion

In conclusion, for the arguments of record and the reasons set forth above, all pending claims of the subject application continue to be in condition for allowance and Appellant seeks the Board's concurrence at this time.

Respectfully submitted,

By: _____

Date: January 21, 2011

John G. Posa
Reg. No. 37,424
Gifford, Krass, Sprinkle, Anderson & Citkowski, P.C.
PO Box 7021
Troy, MI 48007-7021
(734) 913-9300

APPENDIX A

CLAIMS ON APPEAL

1. A secure transaction method, comprising the steps of:

establishing an electronically accessible verification site authorized by the holder of a credit card;

receiving a request for goods or services by a merchant using the credit card, but wherein the card is not required to be physically presented to the merchant;

accessing the verification site by the merchant to determine whether the request for goods or services is an authorized transaction;

sending an electronic authorization communication by the verification site to the holder of the credit card, the message including information indicative of the transaction; and

transmitting, by the holder of the credit card, an approval communication if the transaction is approved by the card holder.

2. The method of claim 1, wherein the verification site is an electronic mail account.

3. The method of claim 2, wherein the electronic mail account was established by the merchant.

4. The method of claim 1, wherein an authorization message is sent from the site to the merchant in response to the step of accessing the verification site by the merchant.

5. The method of claim 4, wherein the authorization message is automatically generated.

6. The method of claim 4, wherein the authorization message is manually generated within a predetermined period of time.

7. The method of claim 4, wherein request for goods or services, the step of accessing the verification site, the authorization message, or any combination thereof, are encrypted.

8. The method of claim 7, wherein the encryption is implemented using an algorithm specific to the holder or an authorized user of the card.

9. The method of claim 4, wherein request for goods or services, the step of accessing the verification site, the authorization message, or any combination thereof, include routing information for future use.

10. The method of claim 1, wherein the step of accessing the verification site by the merchant causes an icon or window to appear in a web browser.

11. The method of claim 1, wherein the verification site is wirelessly accessible.

12. The method of claim 11, wherein the site is accessible through a cellular telephone, personal digital assistant, or other mobile device.

13. The method of claim 1, wherein the information indicative of the transaction includes information identifying the merchant.

14. The method of claim 1, wherein the information indicative of the transaction includes information identifying the goods or services.

15. The method of claim 1, wherein the information indicative of the transaction includes the cost of the transaction.

APPENDIX B

EVIDENCE

1. BPAI Decision dated May 24, 2010.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte BARRY H. SCHWAB and JOHN G. POSA

Appeal 2009-001262
Application 09/877,596
Technology Center 2400

Decided: May 24, 2010

Before, JOHN A. JEFFERY, JOSEPH L. DIXON, and JEAN R. HOMERE, *Administrative Patent Judges.*

Opinion for the Board filed by DIXON, *Administrative Patent Judge.*

Opinion Concurring filed by JEFFERY, *Administrative Patent Judge.*

DECISION ON APPEAL

STATEMENT OF THE CASE

Appellants seek our review under 35 U.S.C. § 134 of the Examiner's final decision rejecting claims 1-12. We have jurisdiction over the appeal under 35 U.S.C. § 6(b).

We AFFIRM.

BACKGROUND

Appellants' invention is directed to a method for secured transactions conducted over computer networks (Spec. 1).

Claim 1 is illustrative:

> 1. A secure transaction method, comprising the steps of:
>
> establishing an electronically accessible verification site authorized by the holder of a credit card;
>
> receiving a request for goods or services at a merchant location using the credit card, but wherein the card is not physically presented to the merchant; and
>
> accessing the verification site by the merchant to determine whether the request for goods or services is legitimate.

The Examiner relies on the following prior art references as evidence of unpatentability:

Khidekel	US 2001/0027527 A1 (effective filing date,	Oct. 4, 2001 Feb. 25, 2000)
Messner	US 2001/0051902 A1	Dec. 13, 2001 Filed Jun. 8, 2001

Appellants appeal the following rejections:

1. Claims 1-4 and 7-12 stand rejected under 35 U.S.C. § 102(e) as anticipated by Khidekel.

2. Claims 5 and 6 stand rejected under 35 U.S.C. § 103 (a) as unpatentable over Khidekel and Messner.

APPELLANTS' CONTENTION

Appellants contend that both inventors have submitted affidavits testifying that a disclosure document was transmitted from inventor Schwab to inventor Posa on February 20, 2000, five days earlier than the effective filing data of the Khidekel reference. Thus, Khidekel can not be qualified as a prior art reference. App. Br. 2.

ISSUE

Has the Examiner erred in finding that the affidavit submitted by one of the inventors lacks proper execution to antedate the cited reference Khidekel?

PRINCIPLES OF LAW

35 U.S.C § 102(e) rejection can be overcome by antedating the filing date of the reference by submitting an affidavit or declaration under 37 C.F R. 1.132 . . . . *In re Mathews*, 408 F.2d 1393 (CCPA 1969).

FACTUAL FINDINGS

1. We adopt the Examiner's findings in the Answer and Final Rejection as our own (Ans. 2 ¶2, Final 2 ¶2).

2. We find that Mr. Schwab filed an original affidavit on December 3, 2004. We find the original affidavit was not made under oath before a notary public, magistrate, or officer authorized to administer oaths.

We find that the copy submitted with the Appeal Brief was a copy of the originally executed affidavit.

3. We find that Mr. Posa filed an affidavit on September 15, 2005 under oath before a notary public. The affidavit declares that Mr. Posa was a co-inventor of the instant invention.

ANALYSIS

Appellants contend that "[b]oth the inventors have submitted affidavits testifying to the fact that a disclosure document was transmitted from inventor Schwab to inventor Posa on February 20, 2000," (App. Br. 2) and "[a]s both affidavits are signed under oath, these should be taken as facts in support of the requisite evidence to establish diligence." (App. Br. 3).

We disagree with the Appellants' contentions. We agree with the Examiner's finding that there is lack of proper execution on the affidavit by Mr. Schwab (FF 1 and FF 2). In addition, even though MPEP § 715.04 I(B) allows to accept the affidavit filed by only one of two joint inventors who is the sole inventor for a claim or claims under a rejection, we only find that Mr. Posa is co-inventor for all claims (FF 3) and therefore both affidavits are required.

Accordingly, we find Mr. Schwab's affidavit is defective, and we find no other substantive arguments in the record to show error in the Examiner's rejections under 35 U.S.C. § 102(e) and 35 U.S.C. § 103(a). Therefore, we sustain the Examiner's rejections under 35 U.S.C. § 102(e) and 35 U.S.C. § 103(a).

DECISION

We affirm the Examiner's § 102(e) rejection of claims 1-4 and 7-12 as anticipated by Khidekel.

We also affirm the Examiner's § 103 rejection of claims 5 and 6 as unpatentable over Khidekel in view of Messner.

TIME PERIOD

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a). *See* 37 C.F.R. § 1.136(a)(1) (2009).

ORDER

AFFIRMED

JEFFERY, Administrative Patent Judge, CONCURRING:

I agree with the majority that the Schwab affidavit is technically defective, and that deficiency is fatal to Appellants' attempt to antedate the Khidekel prior art reference. A harsh result, but one that is nevertheless justified by the procedural infirmities on the record.

Although affidavits (i.e., written statements made under oath) are not required as evidence in this regard, *see* 37 C.F.R. § 1.68; *see also* MPEP § 715.04(II), even if the defective Schwab affidavit could somehow be considered an unsworn declaration, it too would be defective since it lacks the requisite acknowledgment under 35 U.S.C. § 1001 regarding the consequences of willful false statements. *See* MPEP § 715.04(II) (noting that declarations *must* contain this acknowledgment) (emphasis added).

But leaving these procedural technicalities aside, the actual content of both the Schwab and Posa affidavits falls well short of establishing reasonable diligence from conception to constructive reduction to practice which, for purposes of this discussion, I presume to be the filing date of Appellants' provisional application (June 9, 2000).

Even assuming that reasonable diligence need only be shown from the day the disclosure document was communicated (February 20, 2000) to June 9, 2000 (the provisional application filing date), Appellants provide no evidence of such diligence on this record apart from alleging unspecified "discussions and refinements which occurred on a regular basis[.]" *See* Schwab Aff., at ¶ 4; *see also* Posa Aff., at ¶ 5 (same).

Such vague, general statements hardly satisfy the relatively rigorous requirements needed to prove diligence—even during the relatively short

time period between February and June 2000. Simply put, Appellants must account for the *entire* critical time period to show diligence. *Gould v. Schawlow*, 363 F.3d 908, 919 (CCPA 1966) (emphasis added). Indeed, the MPEP is replete with case citations for this very proposition. *See* MPEP 2138.06. Based on these authorities, this record simply falls well short of showing diligence with the requisite particularity.

Therefore, even if the submitted affidavits were properly executed, I would still find them substantively deficient, at least regarding evidencing diligence during the critical period. Nevertheless, I join my colleagues in affirming the Examiner's rejection for the reasons indicated in the majority opinion.

erc

GIFFORD, KRASS, SPRINKLE, ANDERSON & CITKOWSKI, P.C.
P.O.BOX 7021
TROY, MI 48007-7021

APPENDIX C

RELATED PROCEEDINGS

None.